



**First Thought
Independent School**

FIRST THOUGHT CARE SERVICES

Online Safety Policy

2026-2027

Table of Contents

1. AIMS	3
2. LEGISLATION AND GUIDANCE	3
3. ROLES AND RESPONSIBILITIES.....	3
4. EDUCATING PUPILS ABOUT ONLINE SAFETY	6
5. EDUCATING PARENTS/CARERS ABOUT ONLINE SAFETY.....	7
6. CYBER-BULLYING	8
7. ACCEPTABLE USE OF THE INTERNET IN SCHOOL	10
8. PUPILS USING MOBILE DEVICES IN SCHOOL	11
9. STAFF USING WORK DEVICES OUTSIDE SCHOOL	11
10. HOW THE SCHOOL WILL RESPOND TO ISSUES OF MISUSE	11
11. TRAINING	11
12. MONITORING ARRANGEMENTS	12
13. LINKS WITH OTHER POLICIES	12
APPENDIX 1: ACCEPTABLE USE AGREEMENT (PUPILS AND PARENTS/CARERS).....	13
APPENDIX 2: ACCEPTABLE USE AGREEMENT (STAFF, GOVERNORS, VOLUNTEERS AND VISITORS).....	14
APPENDIX 3: ONLINE SAFETY TRAINING NEEDS – SELF-AUDIT FOR STAFF	15
APPENDIX 4: ONLINE SAFETY INCIDENT REPORT LOG	16

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit the user for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and Guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

- [Teaching online safety in schools](#)
- [Preventing and tackling bullying](#) and [cyber-bullying: advice for Head of Schools and school staff](#)
- [Relationships and sex education \(RSE\) and health education](#)
- [Searching, screening and confiscation](#)

It also refers to the DfE's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

3. Roles and Responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the Head of School to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins

and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety and requirements for training and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The governing board will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks and will regularly review their effectiveness. The board will review the [DfE's filtering and monitoring standards](#), and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- Reviewing filtering and monitoring provisions at least annually
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- Having effective monitoring strategies in place that meet the school's safeguarding needs
- The governor who oversees online safety TBC

All governors will:

- Make sure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)
- Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school or college approach to safeguarding and related policies and/or procedures
- Make sure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The Head of School & DSL

The Head of School (who is also the DSL) is responsible for making sure that staff understand this policy, and that it is being implemented consistently throughout the school. They will take lead responsibility for online safety in school, in particular:

- Making sure that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the governing board to review this policy annually and make sure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring

- Making sure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Head of School and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks pupils face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.3 The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Making sure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a fortnightly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Making sure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.4 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and making sure that pupils follow the school's terms on acceptable use (appendix 1)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing
- Following the correct procedures by as advised by the ICT Manager if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to make sure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy

- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of ‘it could happen here’

This list is not intended to be exhaustive.

3.5 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the Head of School of any concerns or queries regarding this policy
- Make sure that their child has read, understood and agreed to the terms on acceptable use of the school’s ICT systems and internet (appendix 1)

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – [UK Safer Internet Centre](#)
- Help and advice for parents/carers – [Childnet](#)
- Parents and carers resource sheet – [Childnet](#)

3.6 Visitors and members of the community

Visitors and members of the community who use the school’s ICT systems or internet will be made aware of this policy and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating Pupils about Online Safety

Pupils will be taught about online safety as part of the curriculum. The school will ensure that online safety is taught as part of a **broad and balanced curriculum**, in line with the *My Digital Skills*, *My PSHE*, and *My Relationships and RSE* frameworks. Teaching will be developmentally appropriate and tailored to the communication needs, sensory profiles, and cognitive levels of all pupils.

4. 1 Informal Pathway (typically pupils with profound and complex needs)

Teaching will focus on building early awareness of safety through supported interaction and adult modelling. Pupils will be taught to:

- Explore the safe use of technology through sensory and cause-and-effect activities.
- Recognise and respond to simple safety cues such as “stop”, “help”, and “no”.
- Understand that familiar adults help to keep them safe when using technology.
- Participate in routines and stories that reinforce safe and respectful interactions with people and devices.
- Develop positive associations with technology as a tool for communication, play, and learning.

Learning will be delivered through **visuals, sensory exploration, repetition, and symbol-supported communication**, in line with PSHE themes of *kindness, personal space, and trusted adults*.

4.2 Semi-formal Pathway (typically pupils with severe learning difficulties or autism)

Teaching will focus on enabling pupils to use technology **safely, respectfully, and responsibly** in familiar contexts. Pupils will be taught to:

- Recognise acceptable and unacceptable behaviour both online and offline.
- Understand the concepts of **public and private** and apply these to digital communication.
- Follow agreed rules for sharing information, photos, and messages safely.

- Identify trusted adults and know how to seek help if they are worried or unsure about something online.
- Recognise examples of online risk (such as pop-ups, strangers messaging, or requests for images) and practise safe responses including *telling an adult* or *turning off the device*.
- Understand that **consent, respect, and kindness** apply equally in online and face-to-face relationships.
- Know that there are **minimum age limits** for social media and that privacy settings help protect personal information.

These skills will be taught through **structured PSHE and RSE lessons**, supported by **visuals, role play, CEOP resources, and social communication activities**.

4. 3 By the end of primary school, pupils will:

- Recognise the importance of kindness, respect, and consent in all interactions, including online.
- Know who to go to for help when they feel unsafe, worried, or upset by something they see online.
- Understand that people may behave differently online and that some individuals may pretend to be someone they are not.
- Be aware that once something is shared online, it can be difficult to remove and may be seen by others.
- Show increasing independence in making safe and responsible choices when using technology.

4. 4 Adaptations for our pupils special educational needs:

Teaching about safeguarding, including online safety, will be **highly individualised**.

Adaptations will include:

- The use of **visual supports, symbols, AAC systems, and sensory resources**.
- Repetition, modelling, and simplified language.
- Personalised teaching about **safe/unsafe, yes/no**, and **public/private** concepts.
- One-to-one or small-group interventions for pupils who require additional support to recognise or respond to unsafe situations.

4. 5 Cross-curricular Links:

The safe and responsible use of technology will be reinforced through:

- **PSHE and RSE** lessons focusing on relationships, consent, and privacy.
- **Communication and life skills** sessions where digital devices are used for expression and interaction.
- **Daily routines** involving photo permissions, device sharing, and supported online communication.
- **Whole-school initiatives** such as *Safer Internet Day* and *Anti-Bullying Week*.

5. Educating Parents/Carers about Online Safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website or virtual learning environment (VLE). This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Head of School who is also the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Head of School.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

The school recognises that pupils with additional learning needs may be especially vulnerable to misunderstanding or distress in online interactions. Preventing cyber-bullying is therefore a key part of our wider safeguarding and emotional-wellbeing work.

Preventive Education

To help prevent cyber-bullying, the school will ensure that pupils:

- Are explicitly taught what **bullying and cyber-bullying** mean in ways that are accessible to their developmental level.
- Learn that **unkind or hurtful behaviour online** can cause the same feelings as unkind behaviour in person.
- Understand that **kindness, consent, and respect** apply to all communication, including messages, photos and online comments.
- Know how to respond if they see or experience unkind behaviour online, including how to **tell a trusted adult** and use **“stop/help” symbols**.

These themes are introduced through the *My PSHE*, *My Relationships and RSE*, and *My Digital Skills* curricula using visuals, social stories, and structured discussion appropriate to each pupil’s communication and comprehension level.

Curriculum Links

Class teachers and support staff will use relevant parts of the curriculum particularly **PSHE, RSE, communication and computing lessons** to explore kindness, respectful communication, and the safe use of technology.

Opportunities will be taken in daily routines, group projects and assemblies to reinforce the message that bullying, including cyber-bullying, is unacceptable.

Staff Training

All staff, governors and volunteers receive **safeguarding and online safety training** that includes the signs, impact and management of cyber-bullying.

Staff are trained to recognise changes in behaviour that may indicate distress from online activity, and to respond calmly and supportively.

Parental Engagement

The school will provide **information for parents and carers** on recognising and responding to cyber-bullying. Guidance will include how to monitor safe technology use at home and how to report concerns to school staff.

Responding to Incidents

Where an incident of cyber-bullying is suspected or reported, the school will follow the procedures set out in the **Behaviour Policy** and **Safeguarding and Child Protection Policy**.

- All reports will be taken seriously and investigated promptly by the class teacher and/or Designated Safeguarding Lead (DSL).
- Support will be offered to both the victim and the pupil(s) involved in the behaviour, recognising the potential for social communication difficulties to contribute to misunderstandings.

- Where illegal, inappropriate or harmful material has been shared, the school will take all reasonable steps to ensure the incident is contained.

If the DSL has reasonable grounds to suspect that the possession or distribution of material is illegal, they will report the incident to the police and provide relevant evidence as soon as practicable. The school will also work with external agencies as required to safeguard all pupils involved.

6.3 Examining electronic devices

The Head of School, and any member of staff authorised to do so by the Head of School as set out in your behaviour policy can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, considering the **risk to the pupil, other pupils, and staff**. If the search is not urgent, they will seek guidance from **the Head of School, DSL, or another senior staff member** before proceeding.
- Take into account the pupil's **communication profile, sensory needs and emotional regulation**, ensuring that the process is calm, supportive and non-confrontational.
- Use **clear, simple language, symbols or visual supports** to explain what is happening and why and offer reassurance throughout.
- Give the pupil time to process information and the opportunity to respond or ask questions in their preferred way.
- Seek the pupil's co-operation and aim to complete the search with minimal distress, using staff who are known to the pupil wherever possible.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so. When conducting a search, staff will ensure that:

- The search is carried out **by at least two members of staff**, one of whom should be a **senior leader or the DSL**, unless the urgency of the situation makes this impossible.
- Wherever possible, a **familiar and trusted adult** is present to support the pupil.
- The search takes place in a **quiet, private area** to reduce distress and sensory overload.
- Staff use **calm, reassuring communication** throughout and avoid physical contact unless absolutely necessary for safety reasons.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are

likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carers refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on [screening, searching and confiscation](#) and the UK Council for Internet Safety (UKCIS) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on [searching, screening and confiscation](#)
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- Our behaviour policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

First Thought Independent School recognises that AI has many uses to help pupils learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

First Thought Independent School will treat any use of AI to bully pupils very seriously, in line with our anti-bullying and behaviour policy.

The school will not be using generative AI.

7. Acceptable use of the Internet in School

All pupils, parents/carers, staff, volunteers and governors are expected to agree to and follow the school's **Acceptable Use Policy** for ICT systems and internet access (see Appendices 1–2).

For pupils, this agreement will be introduced through **visuals, symbols, stories and supported discussion**, ensuring that expectations are understood at an appropriate developmental level. Where pupils are unable to give formal consent, **parents/carers will sign on their behalf**, and staff will continue to reinforce acceptable use through teaching, modelling and daily routines.

Visitors using school equipment or accessing the school network will be expected to read and agree to the school's acceptable use terms, where relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in 21 to 3.

8. Pupils Using Mobile Devices in School

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Tutor group time
- Clubs before or after school, or any other activities organised by the school

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix1).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff Using Work Devices Outside School

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords can be made up of [3 random words](#), in combination with numbers and special characters if required, or generated by a password manager
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by promptly installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 2.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the ICT Manager.

10. How the School will Respond to Issues of Misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

11.1 Staff, governors and volunteers

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
 - Abusive, threatening, harassing and misogynistic messages
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
 - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputy will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

11.2 Pupils

All pupils will receive age-appropriate training on safe internet use as detailed in section 4 of this policy.

Pupils will also receive age-appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

12. Monitoring Arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4.

This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the governing board. The review (such as the one available [here](#)) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with Other Policies

This online safety policy is linked to our:

- Safeguarding and Child protection policy

- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1: Acceptable Use Agreement (Pupils and Parents/Carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET:
AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

At our school, we use computers, tablets, switches and other digital devices to help us learn, play and communicate safely.

When I use school computers, iPads or the internet, I will try to:

- Use my device **with an adult or when an adult says it's OK**.
- Be **kind and gentle** when I use technology or talk to people online.
- Tell an adult straight away if:
 - I see or hear something that makes me worried or upset.
 - I get a message from someone I don't know.
 - Something stops working or breaks.
- Keep my **hands, words and pictures safe** no hurting, shouting or sharing unkind things.
- Use only the websites, apps or games my teacher shows me.
- Ask an adult before taking or sharing a photo or video.
- Look after school equipment carefully and **tell an adult if something is wrong**.
- Keep my passwords private (adults will help me remember them if I need to).
- Stop using the device and ask for help if I feel worried or unsure.

My teachers and adults will help me learn how to stay safe, kind and respectful when I use technology.

I understand that the school checks how devices are used to help keep everyone safe.

Signed (pupil):

Where pupils are unable to sign, staff may record their participation using symbol choice, AAC, or observation of understanding.

Date:

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet and will make sure my child understands these.

Signed (parent/carer):

Date:

Appendix 2: Acceptable use Agreement (staff, governors, volunteers and visitors)

**ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET:
AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS**

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way that could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me, they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):

Date:

Appendix 3: Online Safety Training Needs – Self-audit for Staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 4: Online Safety Incident Report Log

ONLINE SAFETY INCIDENT LOG

Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident